User Manual

iStorage®
SECURING THE MAINSTREAM

datAshur®

2013 UK IT INDUSTRY AWARDS
bcs The Chartered Institute for IT computing
WINNER

FIPS
Level 3 Certified
140-2
Certificate number 1873

Remember to save your PIN in a safe place. If lost or forgotten, there is no way to access the datAshur.

If you are having difficulty please refer to this complete user manual which is loaded on your datAshur and is also available at iStorage's website: www.istorage-uk.com/support

datAshur®

iStorage®
SECURING THE MAINSTREAM

Copyright © iStorage, 2013. All rights reserved.

Windows is a registered trademark of Microsoft Corporation.
All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID

iStorage shall not be liable by virtue of this warranty, or otherwise, for any incidental, special or consequential damage including any loss of data resulting from use or operation of the product, whether or not iStorage was apprised of the possibility of such damages

iStorage datAshur is developed and manufactured by iStorage Limited and is based on DataLock® technology licensed from ClevX, LLC.

FC CE RoHS

All trademarks and brand names are the property of their respective owners.

Table of Contents

Introduction 4

Package contents 4

1. datAshur Layout 5
2. LED Indicators and their actions 5
3. How to change the User PIN 5
4. How to create a new User PIN 6
5. How to unlock the datAshur with a User PIN 8
6. How to lock the datAshur 8
7. How to create an Admin PIN 8
8. How to unlock with Admin PIN 10
9. How to change Admin PIN 11
10. How to reset the datAshur 12
11. How to configure the datAshur with Windows OS 12
12. How to configure the datAshur with Mac OS 15
13. Brute Force Hacking Detection 16
14. FAQ's - Frequently asked questions 17
15. Technical Support 21
16. Warranty and RMA information 21

datashur®

iStorage®
SECURING THE MAINSTREAM

Introduction

Note: The datAshur rechargeable battery is not fully charged, we recommend the battery be charged prior to first use. Please plug in the datAshur drive to a powered USB port for 60 minutes to fully charge the battery.

Thank you for purchasing the iStorage datAshur®, an ultra secure and easy to use, hardware encrypted USB PIN activated flash drive.

The datAshur uses military grade CBC-AES 256-bit hardware encryption, which encrypts all data stored on the drive in real-time. The datAshur requires no software and is OS and host independent.

The datAshur incorporates a rechargeable battery allowing the user to enter a 7-15 digit PIN (Personal Identification Number) onto the on-board keypad before connecting the drive to a USB port.

Should the drive be lost or stolen, the user can rest assured that all data held on the datAshur is safe and cannot be accessed by any unauthorised person.

The datAshur can be configured with both a User and Admin PIN, making it perfect for corporate and government deployment. As the datAshur is unlocked via the onboard keypad and not a host computer, it is not vulnerable to software/hardware based key-loggers or brute force attacks.

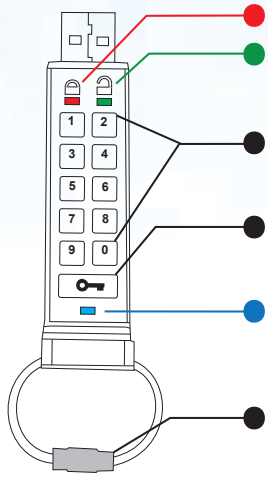
Caution: The datAshur is shipped with a default User PIN of 1-1-2-2-3-3-4-4 and although it can be used straight out of the box with the default PIN, for security reasons, we **highly recommend** that a new User PIN be created immediately by following instructions under section 3 “How to change User PIN”.

If you forget your User PIN and no Admin PIN exists, or you forget both PINs, all data will be inaccessible.

Package contents

- iStorage datAshur drive
- Extruded Aluminium Sleeve
- QSG - Quick Start Guide

1. datAshur Layout



- **Lock** LED, stand by with the datAshur locked
- **Unlock** LED, datAshur is unlocked when flashing
- **Keypad**
- **Key** Button, used to activate the datAshur and to enter PIN codes
- **Blue** LED, when on, the datAshur is connected to the computer. when flashing data is being transferred
- **Keyring**, unscrew to add to key ring.

2. LED indicators and their actions

When all LEDs are OFF the datAshur is locked and secure.					
	blink	Drive is unlocked in **User Mode**		blink	Drive is locked and secure
	double blink	Drive is unlocked in **Admin Mode**		solid	No **User PIN** is configured
	solid	Drive is connected to a powered USB port	&	blink together	Accepting **User PIN** verification when setting / changing the **PIN**
	solid	Drive is connected to host computer and is idle	&	double blink	Accepting **Admin PIN** verification when setting / changing the **PIN**
	blink	Data exchange with host computer	&	illuminate together	Accepting new **PIN**
			&	blink alternately	Error

3. How to change the User PIN

Unless otherwise noted, all steps are performed when datAshur is NOT connected to a computer.

Caution: The datAshur is shipped with a default User PIN of 1-1-2-2-3-3-4-4 and although it can be used straight out of the box with the default PIN, for security reasons, we **highly recommend** that a new User PIN be created immediately by following instructions under section 3 “How to change User PIN”.

If you forget your User PIN and no Admin PIN exists, or you forget both PINs, all data will be inaccessible.

User PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- datAshur must NOT be connected to a host

INSTRUCTIONS	LED ACTIVITY
Press **KEY Button**	& will blink together
Enter **User PIN** to unlock drive (Factory default **PIN** 1,1,2,2,3,3,4,4) and press **KEY Button**	& will illuminate together for approximately 4 seconds and then: will blink indicating correct **PIN** entry
Press and hold **KEY Button** for 3 seconds	& will illuminate together
While & illuminated enter **New User PIN** and press **KEY Button**	& will blink in unison
Re-enter **New User PIN** and press **KEY Button**	& will illuminate and then change to blinking
Insert datAshur into USB port	**N.B.** blinks if 1st and 2nd entries match & blink alternately if **PIN** entry incorrect

Note: If a mistake was made while defining a new PIN or the procedure was not completed, the drive will retain the old PIN.

4. How to create a new User PIN

When all cryptographic parameters have been zeroed.

All cryptographic parameters (including **User PIN** and **Admin PIN**) are zeroed:

- After hacking detection has been triggered by 10 consecutive failed attempts to unlock,
- When the datAshur has been manually reset (see section 11 “How to Reset the datAshur”).

This state is evident by a solid lit **RED LED** indicator. It will be necessary to set a New User PIN by following these instructions.

When either of the above two scenarios occur, it will be necessary to set a new **User PIN** by following the instructions below.

User PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- datAshur must NOT be connected to a host

Password Tip: You can create a word, name, phrase or any other Alphanumerical PIN combination by simply pressing the key with the corresponding letters on it.

Examples of these types of Alphanumerical PINs are:

- For "**Password**" you would press the following keys:
  7(pqrs) **2**(abc) **7**(pqrs) **7**(pqrs) **9**(wxyz) **6**(mno) **7**(pqrs) **3**(def)
- For "**iStorage**" you would press:
  4(ghi) **7**(pqrs) **8**(tuv) **6**(mno) **7**(pqrs) **2**(abc) **4**(ghi) **3**(def)

Using this method, long and easy to remember PIN CODES can be created.

INSTRUCTIONS	LED ACTIVITY
Press and hold **KEY Button** for 3 seconds	& will illuminate together
While & are illuminated enter a **New User PIN** and press **KEY Button**	& will blink in unison
Re-enter **New User PIN** and press **KEY Button**	& will illuminate together for approximately 4 seconds and then: will blink indicating correct **PIN** entry
Insert datAshur into USB port	will illuminate in a constant state & blink alternately if **PIN** entry incorrect

Note: It becomes necessary to format the datAshur at this point as all previous data is obscured with the previous encryption key (including the file allocation table).

A User PIN can only be created when the **RED LED** is lit in a constant state (**reset**) or changed when the **GREEN LED** is blinking (**unlocked**).

Neither **User** nor **Admin PIN** can be created while the drive is connected to a host computer.

5. How to unlock the datAshur with a User PIN

Once the User PIN is created, all data stored on the datAshur is encrypted, in hardware, to the CBC-AES 256-bit specification. In order to access the data stored on the drive, you must first unlock the drive with your User PIN.

INSTRUCTIONS	LED ACTIVITY
Press **KEY Button**	& will blink together
Enter **User PIN** to unlock drive (Factory default **PIN** 1,1,2,2,3,3,4,4) and press **KEY Button**	& will illuminate together for approximately 4 seconds and then: will blink indicating correct **PIN** entry
Note that at this point the following occurs:	will blink indicating the correct **PIN** entry will blink indicating the incorrect **PIN** entry
Insert your datAshur into USB port	will illuminate in a constant state will illuminate and flicker

Note: Once unlocked, the **Green LED** will blink for 30 seconds, within which time the drive needs to be connected to the USB port. If no connection is detected within 30 seconds, the drive will lock and you will need to start the process of unlocking again.

6. How to lock the datAshur

The iStorage datAshur automatically locks when unplugged from the host computer or power to the USB port is turned off. Data is kept locked using CBC-AES 256-bit encryption.

7. How to create an Admin PIN

An Admin PIN is a useful feature for corporate deployment, for example:

- Recovering data from the datAshur and configuring a new User PIN in the event an employee has forgotten their PIN
- Retrieving data from the datAshur if an employee leaves the company

Caution: Entering the Admin PIN to access a locked drive will clear the User PIN. If a user forgets their PIN, access to their drive is regained by defining a new user PIN. For security reasons, we **highly recommend** that a new User PIN be created immediately once the drive has been unlocked using the Admin PIN.

Admin PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- datAshur must NOT be connected to a host

If the datAshur has been reset or hacking detection has been triggered (i.e. no User or Admin PIN exist), the instructions below can be followed. If a User PIN already exists, the datAshur must be unlocked first with the user PIN by following instructions under section 5, before an Admin PIN can be created by following instructions below.

The following table depicts the possible actions when the drive is in different states:

User PIN	Admin PIN	Possible Actions
NOT SET	NOT SET	Can set either **User** or **Admin PIN**
		Cannot access drive until **User** or **Admin PIN** is defined
SET	NOT SET	Can change **User PIN** when unlocked as User
		Can set **Admin PIN** when unlocked with **User PIN**
		Can access data when unlocked as User
NOT SET	SET	Can set **User PIN** when drive is locked
		Can unlock drive with **Admin PIN**
		Can change **Admin PIN** when unlocked as Administrator
		Can perform Administrator commands
SET	SET	Can unlock drive with either **User** or **Admin PIN**
		Can change **User PIN** when unlocked as User
		Can change **Admin PIN** when unlocked as Administrator

The drive has to be unlocked in User mode in order to proceed with configuring an Admin PIN.
It is set by following the instructions below:

INSTRUCTIONS	LED ACTIVITY
Double press the **KEY Button** and hold on the 2nd press for 3 seconds	& will double blink once and then turn solid
Enter the **New Admin PIN** and press **KEY Button**	& will double blink if correct **PIN** entry or will blink alternately if **PIN** entry incorrect
Re - Enter the **New Admin PIN** and press **KEY Button**	& will illuminate together for approximately 2 seconds and then: will double blink indicating correct **PIN** entry
Note that at this point the following occurs:	will double blink if 1st and 2nd entries match & will blink alternately if **PIN** entry incorrect
Insert your datAshur into USB port	will illuminate in a constant state will illuminate and flicker

Note: A **double blink** indicates the drive is unlocked in **Admin mode**.
A **single blink** indicates the drive is unlocked in **User mode**.

Figure 1 shows the **GREEN** blinking characteristics when the drive is opened in User mode (top - single blink) and Admin mode (bottom - double blink).

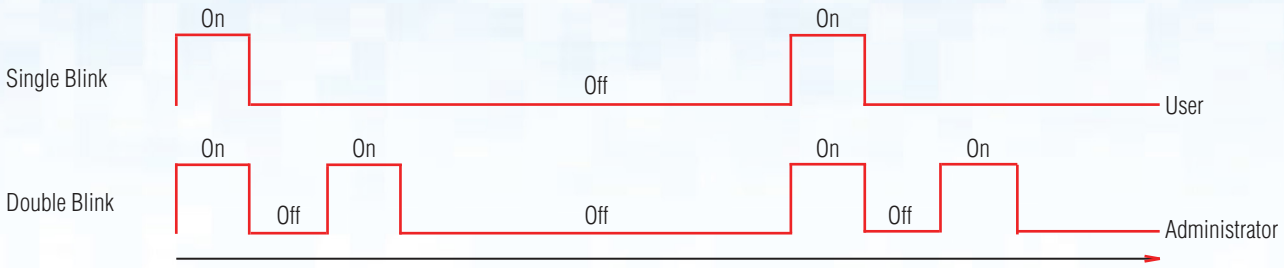


Figure 1: Mode indication

Figure 2 shows the difference between pressing **KEY Button** to set a **User PIN** vs. setting the **Admin PIN**.

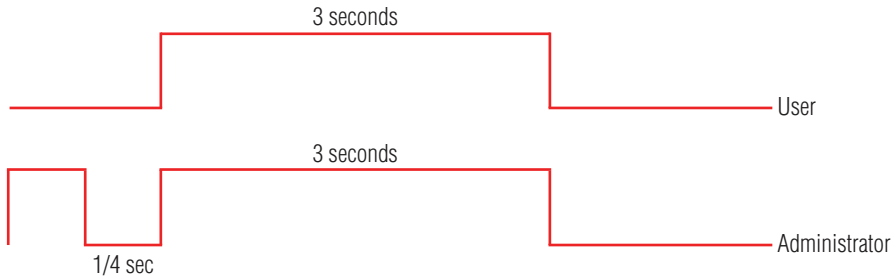


Figure 2: Key entry for mode selection

8. How to unlock with Admin PIN

Caution: Entering the Admin PIN to access a locked drive will clear the User PIN. If a user forgets their PIN, access to their drive is regained by defining a new user PIN. For security reasons, we **highly recommend** that a new User PIN be created immediately once the drive has been unlocked using the Admin PIN.

INSTRUCTIONS	LED ACTIVITY
Press the **KEY Button** twice in succession (similar to double-clicking a mouse)	& will double blink together (Figure 1. above)
Enter **Admin PIN** Press **KEY Button**	& will illuminate together as self-tests are run will double blink if admin entered correct **PIN** will blink if incorrect **PIN** was entered

Note: Once unlocked, the **GREEN LED** will double blink for 30 seconds, within which time the drive needs to be connected to a USB port. If no connection has been detected within 30 seconds the drive will lock.

9. How to change Admin PIN

Caution: Entering the Admin PIN to access a locked drive will clear the User PIN. If a user forgets their PIN, access to their drive is regained by defining a new user PIN. For security reasons, we **highly recommend** that a new User PIN be created immediately once the drive has been unlocked using the Admin PIN.

Admin PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- datAshur must NOT be connected to a host

Once an Admin PIN has been created, the datAshur needs to be unlocked by the administrator in order to change the Admin PIN. The Admin PIN cannot be changed from the User mode.

INSTRUCTIONS	LED ACTIVITY
Press the **KEY Button** [🔑] [🔑] **twice** in succession (similar to double-clicking a mouse)	🔴 & 🟢 will double blink together
Enter **Admin PIN** Press **Key Button** [🔑]	🔴 & 🟢 will illuminate together as self-tests are run 🟢 will double blink if admin entered correct **PIN** 🔴 will blink if incorrect **PIN** was entered
Double press the **KEY Button** [🔑] [🔑] and hold on the 2nd press for 3 seconds	🔴 & 🟢 will double blink once and then turn solid
Enter the **New Admin PIN** and press **KEY Button** [🔑]	🔴 & 🟢 will double blink if correct **PIN** entry or will blink alternately if **PIN** entry incorrect
Re-enter the **New Admin PIN** and press **KEY Button** [🔑]	🔴 & 🟢 will illuminate together for approximately 2 seconds and then: 🟢 will double blink indicating correct **PIN** entry
Note that at this point the following occurs:	🟢 will double blink if 1st and 2nd entries match 🔴 & 🟢 will blink alternately if **PIN** entry incorrect
Insert your datAshur into USB port	🟢 will illuminate in a constant state 🟦 will illuminate and flicker

Note: The **GREEN LED** will double blink for 30 seconds, within which time the drive needs to be connected to a USB port. If no connection has been detected within 30 seconds, the drive will lock.

10. How to Reset the datAshur

In the event both **Admin** and **User PIN** have been forgotten, or user wants to delete all stored data, please follow the instructions below:

The reset process will clear all cryptographic parameters including both **User** and **Admin PIN**. This means a new User PIN will have to be defined in order to re-enable the drive. Also, since this will force the creation of a new encryption key, the datAshur will have to be reformatted (see section 11 or 12).

⚠ **Caution:** Resetting the datAshur will make all data on the drive inaccessible forever.

INSTRUCTION	LED ACTIVITY
Press and hold **KEY Button** & number button together for 3 seconds	& will illuminate together
Release buttons	& will blink in unison
Enter 9 9 9	& will blink in unison
Press **KEY Button**	& will turn off
Press **KEY Button**	will remain in solid state Indicates **User PIN** must be set prior to use

11. How to configure the datAshur with Windows OS

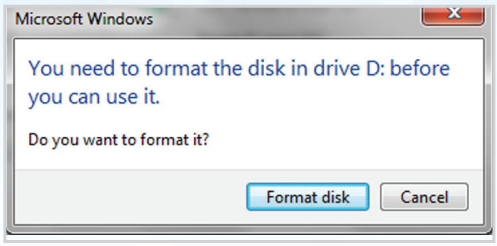
In the event that hacking detection has been triggered by entering the **incorrect PIN 10 times** in succession or the drive has been **reset**, all **data on the drive will be lost forever**.

Once a **New User PIN** has been created, the datAshur will need to be initialised and formatted.

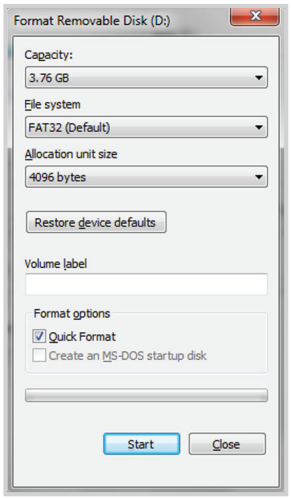
To initialise your datAshur, do the following:

1. Create a **New User PIN** (see section 4).
2. Unlock the datAshur by entering the **New User PIN** and connect to a computer's USB port.

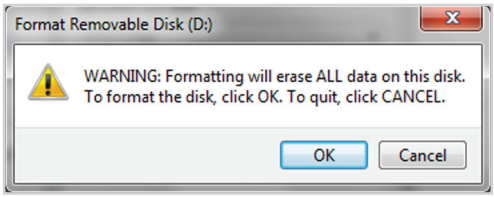
3. The computer should notify the user with the following message:



4. Proceed by clicking on **Format** disk.
Select **FAT32** or **NTFS** depending on your needs, enter a **Volume Label** and click **Start**.

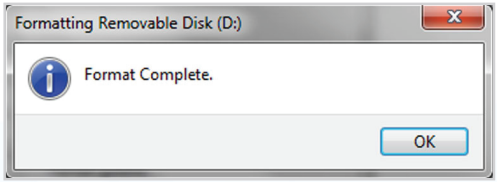


5. Click **OK** to continue with formatting the drive.


Format Removable Disk (D:)
WARNING: Formatting will erase ALL data on this disk.
To format the disk, click OK. To quit, click CANCEL.
OK
Cancel

Warning: This procedure will erase ALL data on the drive.

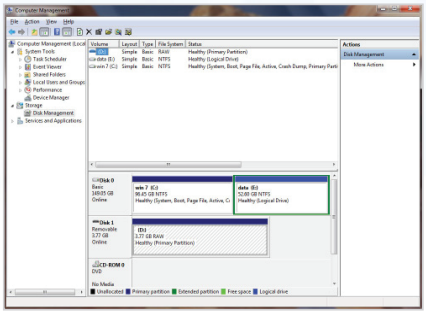
6. The procedure will finish formatting the drive and confirm that formatting has been completed.
While the datAshur is formatting the **BLUE LED** will be flashing.



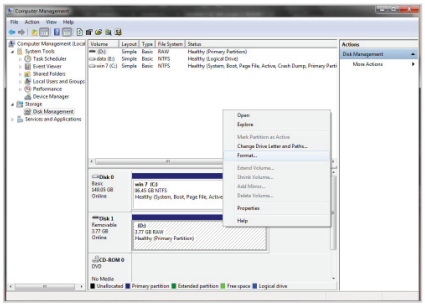
Once finished, the **BLUE LED** becomes solid and your datAshur is ready for use.

In case that the formatting wizard does not appear, please follow the procedure below:

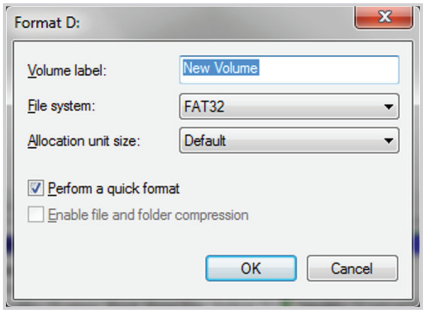
1. Right click **My Computer** or **Computer** and then click **Manage**.
2. In the Computer Management window under the **Disk Management** tab, the datAshur is recognised as a removable device in raw format.



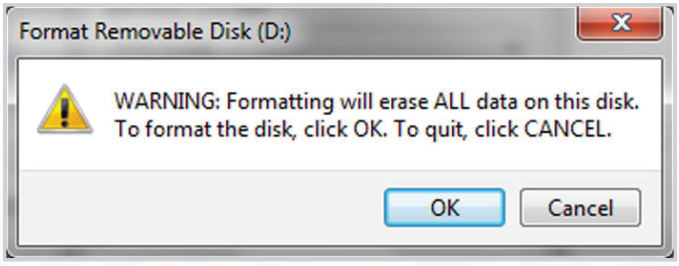
3. In the blank area under the unallocated section right click **Removable Raw Drive** and select **Format.**



4. The Format window will open.
   Enter a new **Volume Label**.
   Select **FAT32** or **NTFS** depending on your needs and click OK.



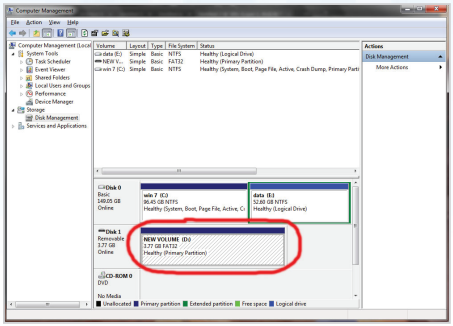
5. Click **OK** on the **Format** warning window to continue with formatting the drive.


Format Removable Disk (D:)
WARNING: Formatting will erase ALL data on this disk.
To format the disk, click OK. To quit, click CANCEL.
OK
Cancel

Warning: This procedure will erase ALL data on the drive.

6. The procedure will finish formatting and return to the **Disk Management** window.

   While the datAshur is formatting the **BLUE LED** will start flashing.



When finished, the **BLUE LED** becomes solid and your datAshur is ready for use.

12. Configure the drive with Mac OS

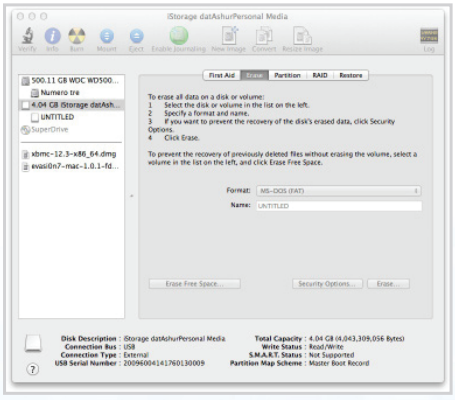
In the event that hacking detection has been triggered by entering the **incorrect PIN 10 times** in succession or the drive has been reset, all **data on the drive will be lost forever**.

Once a **New User PIN** has been created, the datAshur will need to be initialised and formatted.

To format your datAshur on Mac OS computers, do the following:

1. Create a **New User PIN** (see section 4).
2. Unlock the datAshur by entering the **New User PIN** and connect to a Mac computer's USB port.
3. The system will prompt you with **INITIALIZE** window.

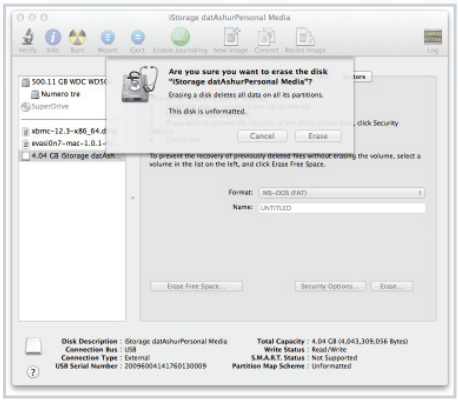
4. Press **INITIALIZE** and select the datAshur in the Disk Utility window.



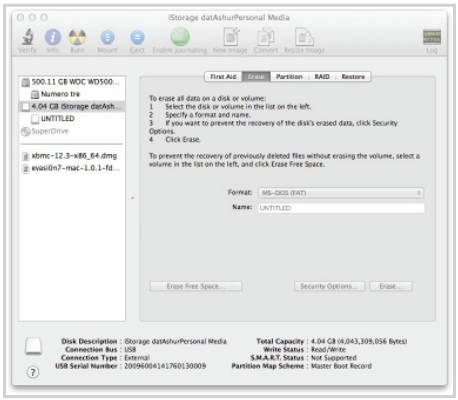
iStorage datAshur® Manual v 3.1

To format your datAshur on Mac OS computers, do the following:

5. Click on the datAshur on the left side of the **Disk Utility** window.
6. Choose **Erase** from the contextual menu on the right side of the window.
7. Select **MS-DOS** for the **Volume Format**.
8. Click **Erase**.



9. The formatted datAshur will appear in the **Disk Utility** window and will mount onto the desktop.



13. Brute Force Hacking Detection

After 10 consecutive incorrect PIN attempts, the following occurs:

- All cryptographic parameters are zeroed
- The User and Admin PINs are deleted
- All data previously stored on the drive will be lost forever

The datAshur, unlike other similar drives, is preprogrammed with an unlimited number of randomly generated encryption keys. Each time hacking is detected (i.e. the wrong PIN is entered a total of 10 consecutive times), all cryptographic parameters are zeroed including User and Admin PIN. Once a new User PIN is created the drive randomly generates a new encryption key. Because of this, the datAshur will have to be formatted after each time the defence mechanism is triggered.

14. FAQ's - Frequently Asked Questions

Caution: There are no "**Back Doors**" to our products, we cannot retrieve a forgotten PIN or retrieve any data off the drives unless the PIN is known.

We strongly recommend that you carefully read this User Manual, shipped with the device or available for download on our website before contacting us for technical support.

Below are answers for the most frequently asked questions:

Q. HOW DO I USE THE datAshur FOR THE FIRST TIME?

A. The datAshur comes with a default User PIN which will unlock the device for the first time, allowing the user to create their own unique User and Admin PIN.

Please follow this procedure:

Press **KEY** Button
Enter **1-1-2-2-3-3-4-4**
Press **KEY** Button
The **GREEN** **LED** light will indicate the device is unlocked

Q. WHAT IS A USER PIN CODE?

A. The User PIN (Personal Identification Number) can be changed to almost any number that is desired.

To create your New User PIN refer to section 4 on page 6 and follow the guidelines below:

Must be between 7-15 digits in length
Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
datAshur must NOT be connected to a host

Password Tip: You can create a word, name, phrase or any other Alphanumerical PIN combination by simply pressing the key with the corresponding letters on it.

Examples of these types of Alphanumerical PINs are:

- For "**Password**" you would press the following keys:
  7(pqrs) **2**(abc) **7**(pqrs) **7**(pqrs) **9**(wxyz) **6**(mno) **7**(pqrs) **3**(def)
- For "**iStorage**" you would press:
  4(ghi) **7**(pqrs) **8**(tuv) **6**(mno) **7**(pqrs) **2**(abc) **4**(ghi) **3**(def)

Using this method, long and easy to remember PIN CODES can be created.

Q. HOW DO I UNLOCK THE datAshur IF THE BATTERY IS DEAD?

A. Your datAshur has a built-in rechargeable battery. Even if the battery is fully discharged you can still continue to use the drive by following the instructions below:

Connect the datAshur to a USB port on any computer
While connected to the computer, enter the User or Admin PIN to unlock the drive
While connected to the USB port, the internal battery will automatically charge - this is shown by a flashing **BLUE** **LED**.

We recommend you keep the datAshur connected for approximately 1 hour to fully charge the battery.

Q. HOW DO I CHANGE THE DEFAULT PIN CODE?

A. Please follow this procedure:

Press the **Key** Button
Within 10 seconds enter the Current User PIN and press the **Key** Button again
Press and hold the **Key** Button for 3 seconds
Enter a New User PIN number (The PIN must be 7 - 15 digits long)
Press the **Key** Button to store the New User PIN
Re-enter the New User PIN number
Press the **Key** Button to confirm the New User PIN.

Q. WHAT IF I FORGET MY PIN CODE ON MY datAshur?

A. If you forget the User and Admin PIN, there is absolutely no way of gaining access to the data stored on the drive, there are no back doors into the drive.

You will need to completely reset the datAshur by following the directions in this User Manual. By resetting the drive, all data stored on the datAshur will be deleted.

When the datAshur is reset the following occurs:

- A new encryption key is generated
- The User and Admin PIN are deleted
- All the data on the datAshur is deleted
- A new User PIN will need to be set
- The datAshur will need to be formatted

Q. HOW DO I CREATE AN ADMIN PIN?

A. The Admin PIN is useful in a corporate environment where an Administrator can provide access to the datAshur if the User PIN is forgotten or unavailable.

Please follow this procedure:

Press the **Key** Button
Enter the User PIN within 10 seconds and press the **Key** Button.
Rapidly press the **Key** Button twice and hold the **Key** Button on the second press for 4 seconds.
Enter a new Admin PIN and press the **Key** Button.

NOTE: If the **LEDS** in the above step are "**single blinking**" then the
first key press did not register or was not fast enough.
If you continue, you will be changing the User PIN.
Re-enter the New Admin PIN and press the **Key** Button.

Q. WHAT IS BRUTE FORCE OR HACKING ATTEMPT PROTECTION?

A. 10 consecutive incorrect PIN entries will activate the brute force mechanism and will completely reset the drive as follows:

- A new encryption key is generated.
- The User and Admin PIN are deleted.
- All the data on the datAshur is deleted.
- A new User PIN will need to be set.
- The datAshur will need to be formatted.

Q. HOW DO I RESET THE datAshur?

A. In case the User PIN is forgotten, or if you would like to delete all data stored on the drive and configure a New User PIN, the RESET process will clear the User and Admin PIN, the encryption key and will destroy all data. This means a New User PIN will have to be defined in order to re-enable the datAshur.

Also, since this forces the creation of a new encryption key, the datAshur will have to be reformatted.

Please follow this procedure:

Press and hold the **Key** Button and the number **2** Button for 3 seconds.
Press **9 - 9 - 9** and press the **Key** Button.
Press the **Key** Button again.

NOTE: When the solid **RED** **LED** is on, a New User PIN will need to be set.

Q. HOW DO I CREATE A NEW USER PIN AFTER RESETTING THE datAshur?

A. Once the datAshur has been reset either with the method from the previous step or from a brute force attack (10 unsuccessful attempts to unlock) a New User PIN will need to be defined.

Please follow this procedure:

Press and hold the **Key** Button for 3 seconds.
Within 10 seconds enter the New User PIN.
Press the **Key** Button to save.
Re-enter the New User PIN number & press the **Key** Button.
If the New User PIN was accepted, the **GREEN LED** will be flashing.

The datAshur will be unlocked and be ready to format.

Q. HOW SHOULD I FORMAT MY DRIVE?

A. The datAshur drives come formatted to **FAT32** filing system by default. This will allow you to use the datAshur across all platforms (Windows, Apple, Linux) with a file size limitation of up to 4GB.

Q. WHAT IS THE DIFFERENCE BETWEEN THE USER MODE AND ADMIN MODE?

A. For an ordinary user we recommend to have just one PIN code, whereas in a corporate environment we strongly suggest creating an **Admin PIN** and **User PIN**. When in admin mode you will be able to change the User PIN code.

Q. HOW DO I ACCESS ADMIN MODE?

A. Please follow this procedure:

Press the **Key** Button 2 times.
Within 10 seconds enter the Admin PIN.
Connect the datAshur to a USB port within 30 seconds.

15. Technical Support

iStorage provides the following helpful resources for you:

iStorage's Website
http://www.istorage-uk.com

E-mail correspondence
support@istorage-uk.com

Telephone support with our Technical Support Department on **+44 (0) 20 8991-6260**.
iStorage's Technical Support Specialists are available from 9:00 a.m. to 5:30 p.m.
GMT - Monday through Friday.

16. Warranty and RMA information

Three Year Warranty:

iStorage offers a 3-year warranty on the iStorage datAshur against defects in materials and workmanship under normal use. The warranty period is effective from the date of purchase either directly from iStorage or an authorised reseller.

Disclaimer and terms of warranty:

THE WARRANTY BECOMES EFFECTIVE ON THE DATE OF PURCHASE AND MUST BE VERIFIED WITH YOUR SALES RECEIPT OR INVOICE DISPLAYING THE DATE OF PRODUCT PURCHASE.
ISTORAGE WILL, AT NO ADDITIONAL CHARGE, REPAIR OR REPLACE DEFECTIVE PARTS WITH NEW PARTS OR SERVICEABLE USED PARTS THAT ARE EQUIVALENT TO NEW IN PERFORMANCE. ALL EXCHANGED PARTS AND PRODUCTS REPLACED UNDER THIS WARRANTY WILL BECOME THE PROPERTY OF ISTORAGE.
THIS WARRANTY DOES NOT EXTEND TO ANY PRODUCT NOT PURCHASED DIRECTLY FROM ISTORAGE OR AN AUTHORIzED RESELLER OR TO ANY PRODUCT THAT HAS BEEN DAMAGED OR RENDERED DEFECTIVE: 1. AS A RESULT OF ACCIDENT, MISUSE, NEGLECT, ABUSE OR FAILURE AND/OR INABILITY TO FOLLOW THE WRITTEN INSTRUCTIONS PROVIDED IN THIS INSTRUCTION GUIDE: 2. BY THE USE OF PARTS NOT MANUFACTURED OR SOLD BY ISTORAGE; 3. BY MODIFICATION OF THE PRODUCT; OR 4. AS A RESULT OF SERVICE, ALTERNATION OR REPAIR BY ANYONE OTHER THAN ISTORAGE AND SHALL BE VOID. THIS WARRANTY DOES NOT COVER NORMAL WEAR AND TEAR.
NO OTHER WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OR MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, HAS BEEN OR WILL BE MADE BY OR ON BEHALF OF ISTORAGE OR BY OPERATION OF LAW WITH RESPECT TO THE PRODUCT OR ITS INSTALLATION, USE, OPERATION, REPLACEMENT OR REPAIR.
ISTORAGE SHALL NOT BE LIABLE BY VIRTUE OF THIS WARRANTY, OR OTHERWISE, FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGE INCLUDING ANY LOSS OF DATA RESULTING FROM THE USE OR OPERATION OF THE PRODUCT, WHETHER OR NOT ISTORAGE WAS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

© iStorage, 2013. All rights reserved.
iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, England
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
e-mail: info@istorage-uk.com | web: www.istorage-uk.com